



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/893,501

06/29/2001

Todd Flemming

26509U

6332

20529

7590

04/12/2007

NATH & ASSOCIATES

112 South West Street

Alexandria, VA 22314

EXAMINER

SHIFERAW, ELENI A

ART UNIT

PAPER NUMBER

2136

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
--	-----------	---------------

3 MONTHS

04/12/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

09/893,501

Applicant(s)

FLEMMING, TODD

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 January 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3,5,7-9,13-17 and 19-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3,5,7-9,13-17 and 19-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/29/2007 has been entered.

Claims Status

2. Claims 1-3, 5, 7-9, 13-17, 19-29 are pending, claims 4, 6, 10, 11, and 18 are previously canceled, and all independent claims 1, 12, and 20 are presently amended.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-3, 5, 7-9, 12-17, and 19-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mimura et al. USPN 6,747,564 B1 in view of Johnson et al. USPN 5,349,662 and Fufido et al. USPN 6,720,874 B2.

Regarding claims 1, 12, 20, Mimura et al. discloses the method/system of protecting an asset of an information and/or physical type, comprising

a physical asset protection module that provides physical protection for said asset by triggering a user status change upon valid entry or exit through a door of a building (fig. 1 & 8, col. 4 lines 23-42, and col. 6 lines 48-50, col. 7 lines 18-20, and col. 5 lines 23-37; *smart card door authentication based on user status change...storing staff info. when valid entry, erasing info. when user exits, and storing admission of the staff and verification result to the log file 180*);

an information asset protection module that provides information security protection for said asset (col. 4 lines 22-65; *bank door and bank user database, that stores important customer's information, authentication*); and

an integrator that performs an integration of said physical asset protection module and said information asset protection module, wherein said system is one of in a centrally-located hosted environment (fig. 1 element 185, 125, 150, and 165) and at said asset, the integrator providing integration of the physical protection and information from the information asset protection module to grant rights to the information systems based on physical access, or independently of physical access, wherein the information asset protection reflects the user status change updated to reflect changes in security access requirements (col. 5 lines 50-col. 7 lines 55; *building authentication information result fails access to the computer database log-on is denied i.e. smart card door authentication is integrated with computer database/application authentication*).

Mimura et al. fails to explicitly disclose making access decisions in accordance with usage patterns of the user and wherein usage patterns are calculated by comparing a present usage with historic usage. However Johnson et al. teaches activity detection table/database that stores description of user event activities and a time of occurrence of the user activity indicating events (col. 3 lines 67-col. 4 lines 28) and monitoring user activities (interprocess communications) (col. 4 lines 10-14, and col. 6 lines 39-41) and a decision block that determines whether the interprocess communication is a user activity indicating event described in the user activity event table (col. 6 lines 42-47) and makes a multiple different decisions by comparing current user activities with stored user activities (col. 6 lines 44-64, col. 7 lines 8-37, col. 8 lines 12-68).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of comparing current user activities with previously stored user activities to make a decision within the system of Mimura et al. to monitor user activities and report to a manager/supervisor (see col. 3 lines 16-19). One would have been motivated to modify the teachings because it would control unauthorized access by denying access (see col. 6 lines 55-59).

Mimura et al. and Johnson et al. all the subject matter as described above including the access management device 185 authenticating user access to terminal 165 by comparing temporarily stored staff information with received staff information from terminal 165 and transmitting the verification failure result to terminal 165 when the comparison fails and the terminal 165 generating deny access and an alarm (col. 7 lines 11-28 of Mimura). However the combination fails to explicitly teach a *transmitter* for maintaining information asset protection by

denying access to the information asset in the *centrally-located hosted* environment when there is a breach of the physical asset protection. However Fufido et al. discloses the well-known breach signal transmission from an authenticator of a door 92 that scans door cards to central security control center 68 when access is denied at the door (see col. 8 lines 15-col. 10 lines 38).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Fufido et al. within the combination system because they are analogous in authentication and verification. One would have been motivated to incorporate the teachings because it would alarm an administrator remotely when a breach occurs.

Regarding claim 2, Minura et al. teaches the method, said integrating step comprising providing: maintaining and operating a software application that integrates said physical asset protection and said information asset protection in said hosted environment in accordance with user instructions (col. 4 lines 22-65).

Regarding claim 3, the combination of Minura et al. and Johnson et al. teach the method, further comprising the steps of:

registering a user by storing user information (Minura et al. fig. 20 element 2060);
authenticating a user by comparing at least one user characteristic from said user information with a third-party database; comparing a current asset use pattern with a historical asset use pattern for said user to detect anomalous usage (Minura et al. col. 7 lines 1-65);

updating said historical use pattern on the basis of said current use pattern (Johnson et al. col. 7 lines 8-11);

taking a corrective action, wherein a first corrective action is taken if said authenticating step generates a non-authenticated user output and a second corrective action is taken if anomalous usage is detected during said comparing step (Minura et al. col. 7 lines 1-65); and

wherein said authenticating and comparing steps provide physical asset protection and information asset protection and are performed in said hosted environment (Minura et al. col. 7 lines 1-65).

Regarding claim 5, Minura et al. teaches the method, further comprising the steps of:

registering a visitor by providing initial visitor information (Minura et al. fig. 20 element 2060); comparing said initial visitor information with a third-party database to determine if said registered visitor is entitled to access to said asset; and receiving said registered visitor in an authentication area (Minura et al. col. 7 lines 1-65);

checking a match of said registered visitor with a physical entity (Minura et al. col. 7 lines 1-65); regulating entry on the basis of said checking and comparing steps, wherein said registered visitor is denied access if said registered visitor does not match said physical entity, or said comparing step indicates that said visitor does not have access to said asset (Minura et al. col. 7 lines 1-65); and

wherein at least one of said comparing step, said receiving step and said checking step provide physical asset protection and information asset protection (fig. 1 element 130).

Regarding claim 7, Minura et al. teaches the method, wherein one of said receiving step and said comparing step comprises applying biometrics to control access for said user (fig. 9 element 930).

Regarding claim 8, Minura et al. teaches the method, wherein said biometrics comprises one of scanning and testing a target tissue of said visitor's body (fig. 9 element 930).

Regarding claim 9, Minura et al. teaches the method, wherein said physical asset protection comprises securing ingress and egress areas for a location protected by a physical barrier (fig. 1).

Regarding claim 13, the combination teach the asset protection system, further comprising a user tracking system that authenticates a user as a registered user and provides physical access and information access to said asset in accordance with historical use patterns of said user for said asset, wherein said user tracking system updates said historical use patterns in accordance with a current use pattern of said user (Minura et al. fig. 9 and Johnson claim 1).

Regarding claim 14, Minura et al. teaches the asset protection system, said historical use patterns comprising at least one of frequency, type and time duration (claim 1).

Regarding claim 15, Minura et al. teaches the asset protection system, further comprising a visitor tracking system that authenticates a registered visitor that has not been barred from

Art Unit: 2136

accessing said asset, and allows access in accordance with reception authentication process (fig. 1).

Regarding claim 16, Minura et al. teaches the asset protection system, further comprising a biometrics authentication subsystem that uses physical data of said visitor to allow said access (fig. 9 element 930).

Regarding claim 17, Minura et al. teaches the asset protection system, wherein said physical data comprises a test data portion of said visitor's body (fig. 9 element 930).

Regarding claim 19, Minura et al. teaches the asset protection system wherein said integration is performed in response to an instruction to develop, maintain and operate a computer application to protect said asset (col. 2 lines 28-64).

Regarding claim 21, Minura et al. teaches the method, wherein said transmitting step comprises: providing user registration information to said hosted environment (fig. 5); and processing at said hosted environment said user information to generate said second signal (col. 7 lines 11-28).

Regarding claim 22, Minura et al. teaches the method, wherein said receiving step comprises receiving an access decision from said hosted environment, said decision being in accordance with biometrics of a user (col. 7 lines 11-28).

Regarding claim 23, Minura et al. teaches the method, further comprising comparing said user information to a third-party database to generate an authentication output as said second signal (col. 7 lines 11-28).

Regarding claim 24, Minura et al. teaches the method, further comprising the steps of: entering credentials of a user into an access database in said hosted environment to enroll said user (fig. 8); and outputting an identification object in accordance with said credentials, wherein unauthorized access is denied by said hosted environment (fig. 8).

Regarding claim 25, Minura et al. teaches the method, said entering step comprising the steps of: providing an authorized operator with permission to at least one of alter and append said access database (col. 5 lines 23-38);

obtaining a biometric from said user and searching for said biometric in said access database to generate a search result, wherein said biometric and credential data is added to said access database if said search result indicates an absence of said biometric, and if said search result indicates a presence of said biometric in said access database, one of verifying said credential data if said user is authentic and denying access to said user if said user is not authentic, in accordance with said biometric (fig. 9);

denying access to said user if said user appears in a barred user database (fig. 23);
determining if a photo of said user is in said hosted environment, wherein a digital image is imported to generate said photo if said photo is not present in said hosted environment; verifying that said photo represents said new user (col. 3 lines 1-12);
providing additional user information and user access privileges to said hosted environment (col. 5 lines 3-21); and
generating said identification object having a predetermined layout, said identification object comprising an encrypted three-dimensional barcode in accordance with said biometric and said credential data (fig. 7 element 820).

Regarding claim 26, Minura et al. teaches the method, said outputting step comprising the steps of:

receiving said identification object from said hosted environment and producing a copy of said identification object (col. 5 lines 23-38);
said user verifying integrity of said biometric, said photo and said credentials; and distributing said identification object to said user col. 3 lines 1-12).

Regarding claim 27, Minura et al. teaches the method, wherein said identification object is produced by printing an identification badge (fig. 1 element 200).

Regarding claim 28, Minura et al. teaches the method, wherein said biometric comprises a scan of a biological target tissue (fig. 5 element 515).

Regarding claim 29, Minura et al. teaches the method, wherein said target tissue comprises at least one of finger, hand and eye parameter (fig. 5 element 515).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867.

The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

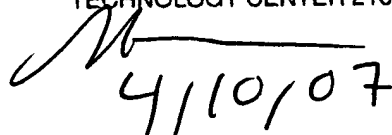
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

3s

April 10, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


4/10/07